UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK

MOOG INC.,

Plaintiff,

v.

SKYRYSE, INC., ROBERT ALIN PILKINGTON, MISOOK KIM, and DOES NOS. 1-50,

Defendants.

Case No.: _____________

MEMORANDUM OF LAW IN SUPPORT OF PLAINTIFF'S MOTION FOR EXPEDITED DISCOVERY

TABLE OF CONTENTS

Page

I. INTRODUCTION 1

II. STATEMENT OF FACTS 2

A. Parties 2

B. Moog's Flight Control Software 2

C. Platform's Immense Value to Moog 3

D. Efforts to Keep Moog's Flight Control Software Secret 4

E. Relevant Moog Team That Developed Platform 6

F. Moog and Skyryse's Initial Business Relationship 6

G. Skyryse's Changes Its Business Model to Overlap with Moog's 7

H. Skyryse's Raiding of Moog's Employees 8

I. Substantial Data Theft of Moog's Most Proprietary Information 9

J. Nature and Value of the Copied Data 10

K. No Legitimate Purpose for Kim's Data Copying 11

L. Kim Returns Two Hard Drives Which are Both Wiped Clean 12

M. Unmanned Helicopter Aviation Market and Barrier to Entry 13

N. Level of Investment by Moog in its Flight Control Programs 14

O. Reputational Harm and Loss of Goodwill 15

III. ARGUMENT 16

A. Good Cause for Expedited Discovery 16

B. Defendants Will Not Be Prejudiced by Expedited Discovery, and Plaintiffs Would Be Prejudiced if Expedited Discovery Were Not Granted 20

IV. CONCLUSION 20

TABLE OF AUTHORITIES

Page(s)

Cases

Asa v. Pictometry Int'l Corp.
757 F. Supp. 2d 238 (W.D.N.Y. 2010) 19

Ayyash v. Bank Al-Madina
233 F.R.D. 325 (S.D.N.Y. 2005) 16

Delphine Software Int'l v. Elec. Arts, Inc.
No. 99 CIV. 4454 AGAS, 1999 WL 627413, at *3 (S.D.N.Y. Aug. 18, 1999) 16, 18

In re Document Techs. Litig.
No. 17-CV-2405, 2017 WL 4350597 (S.D.N.Y. June 27, 2017) 18

Fabkom, Inc. v. R.W. Smith & Assocs., Inc.
No. 95 CIV. 4552 (MBM), 1996 WL 531873 (S.D.N.Y. Sept. 19, 1996) 19

New York by Schneiderman v. Griepp
No. 17CV3706CBAJO, 2017 WL 3129764 (E.D.N.Y. July 20, 2017) 16

OMG Fid., Inc. v. Sirius Techs., Inc.
239 F.R.D. 300 (N.D.N.Y. 2006) 18, 20

Oneida Grp. Inc. v. Steelite Int'l U.S.A. Inc.
No. 17CV0957ADSAKT, 2017 WL 1954805 (E.D.N.Y. May 10, 2017) 16

Philip Morris USA Inc. v. Garrow
No. 8:13-CV-1549 GTS, 2013 WL 6844347 (N.D.N.Y. Dec. 17, 2013) 18

PLC Trenching Co., LLC v. Newton
No. 6:11-CV-0515, 2011 WL 13135653 (N.D.N.Y. Dec. 12, 2011) 19

Secured Worldwide LLC v. Kinney
No. 15 CIV. 1761 CM, 2015 WL 1514738 (S.D.N.Y. Apr. 1, 2015) 19

Stern v. Cosby
246 F.R.D. 453 (S.D.N.Y. 2007) 16

Sylmark Holdings Ltd. v. Silicone Zone Int'l Ltd.
5 Misc. 3d 285 (N.Y. Sup. Ct. 2004) 19

Ticor Title Ins. Co. v. Cohen
173 F.3d 63 (2d Cir. 1999)....................18

United States v. Erie Cnty.
No. 09-cv-849S, 2010 U.S. Dist. LEXIS 144503 (W.D.N.Y. March 6, 2010) 20

<u>Other Authorities</u>

Fed. R. Civ. P. 26(d) 16

Fed. R. Civ. P. 26(f) 16

Fed. R. Civ. P. 30(b)(6)....................17

I. INTRODUCTION

Plaintiff Moog Inc. ("Plaintiff" or "Moog") respectfully submits this memorandum of law in support of its motion for expedited discovery to prepare for the hearing on Plaintiffs' motion for preliminary injunction filed contemporaneously with this motion. As described in Moog's Complaint and Motion for a Temporary Restraining Order/Preliminary Injunction, Moog seeks extraordinary relief to stop one of the most brazen and egregious schemes of trade secret theft in recent memory. This scheme involves a prior business relationship between Moog and Defendant Skyryse, Inc. ("Skyryse") from 2018-2020. As soon as the relationship ended, Skyryse suddenly changed its entire business model to mirror Moog's model, Skyryse raided and hired away over twenty of Moog's senior staff and best software engineers, and a former Moog employee stole over 136,000 files of Moog's most sensitive and proprietary data related to its flight control software (including 43,960 source code files) that took over 15 years to develop, less than one month before leaving Moog and joining Skyryse. Then, as part of a blatant coverup, the hard drive used to copy Moog's data was intentionally wiped clean in such a manner that Moog cannot determine the drive's contents or if any data was copied or transferred to another location or device. If Defendants are not stopped immediately, Moog faces the irreparable loss of business, client relationships and goodwill, as well as the irreversible disclosure of its trade secrets to a direct competitor.

Moog seeks expedited discovery in preparation for the hearing on Moog's Motion for Preliminary Injunction, which is necessary to prevent irreparable harm to Moog. The expedited discovery sought by Moog is necessary, narrowly tailored to the issues presented in Moog's accompanying motion papers, and reasonable under the circumstances. Such discovery would not prejudice Defendants, but Moog would be prejudiced if denied expedited discovery. When, as here, expedited discovery is requested in connection with a preliminary injunction hearing, courts in the Second Circuit uniformly allow such expedited discovery. Moog is entitled to expedited discovery that is solely in Skyryse's possession, including information about: 1) Skyryse's access, use, and/or disclosure of Moog's stolen data; 2) communications between Skyryse or Pilkington and Kim before and after the data theft at issue on November 19, 2021; and 3) communications between Skyryse and Moog's employees while they were working at Moog. Accordingly, there is ample good cause for granting this motion, and for the reasons set forth below, this Court should grant this motion in its entirety.

II. STATEMENT OF FACTS

A. Parties

Founded in 1951 in East Aurora, New York, Moog is a publicly traded (NYSE: MOG.A, MOG.B) aerospace and defense company. Moog designs and manufactures electric, electro-hydraulic and hydraulic motion, controls and systems for applications in three segments: aircraft controls, space and defense controls, and industrial controls. Moog has developed the flight control systems used on some of the most common commercial aircrafts used today, including the Boeing 787 and Airbus A350. Moog works frequently on classified United States government projects, as well as third party commercial projects. Moog has over 10,000 employees and has sales, engineering, and manufacturing facilities in twenty-six countries.

Skyryse, founded in 2016 in Los Angeles, is an aerospace start-up company.

B. Moog's Flight Control Software

Moog designs and manufactures the most advanced motion control products for aerospace, defense, industrial and medical applications. (Hunter Dec., ¶ 5). Moog develops software that governs flight controls for airplanes and other aircrafts, including helicopters. (*Id.*, ¶ 6). Essentially, Moog develops software that pairs up with the hardware computer contained in an aircraft to control its flight and navigation functionality. For example, when a pilot moves a control well in the cockpit, Moog's software reads the control and moves the particular component of the airplane. (*Id*., ¶ 7).

Moog's base flight control software is called Platform. (Hunter Dec. ¶ 8) (Schmidt Dec., ¶ 5). Platform is the "operating system" that an aircraft's computer uses, similar to Windows or Mac OS for a standard home computer. (*Id*.). On top of the base operating system, applications specific to the particular aircraft involved are built and sit on top of the Platform base operating system to tailor its functionality to the particular aircraft. (*Id*.). The particular application provides a specific use, but the underlying operating system allows the entire system and machine to work. (*Id*.). Over the past 15 years, Moog has developed three major branches of the Platform base flight control operating system software: one for commercial aircrafts, one for military use (called "eRTOS"), and one for motor applications (called "AMP"). (Hunter Dec. ¶ 9) (Schmidt Dec. ¶ 6). Building each iteration of the Platform software required 10 full-time software engineers over a period of two to three years. (*Id*.).

C. Platform's Immense Value to Moog

The Platform base software, and related project-specific applications, constitute Moog's most valuable, sensitive, and proprietary information. (Hunter Dec. ¶ 12). The types of information relating to Platform and related project-specific applications that Moog always treats as internal trade secrets which are never disclosed to other parties are: 1) the source code for these programs; and 2) certain documents and checklists prepared by Moog's Software Engineering Process Group ("SEPG"), which contain processes to ensure that the software is being developed in a manner to meet certification requirements by the Federal Aviation Administration ("FAA") and other similar authorities around the world. (*Id*., ¶ 28). The SEPG documents have been optimized over 20 years of working with aviation authorities around the world. (*Id.*). Many companies hire Moog for software development specifically because Moog knows how to efficiently certify software to meet governing aviation standards. (*Id.*).

Platform allows Moog to be a front-runner in obtaining bids from commercial or military parties (*Id.*, ¶ 13). Other competitors do not have this level of adaptable base software which allows project-specific applications to be developed so quickly on top of an existing base software. (*Id.*). On top of the multiple years it took to build Platform, the testing requirements for flight control software are extremely vigorous and costly. (*Id.*, ¶ 15). Before any flight control software is approved by the FAA or similar governing bodies, it must be vigorously tested and certified. (*Id.*). It takes double the resources to certify a flight software than it does to construct it, and this process constitutes two-thirds of Moog's total cost to build flight software. (*Id.*).

If a third party had possession of Moog's Platform software and its underlying code, testing, and certification requirements, the third party company could easily "click and build" a project specific software on top of the base software in a short amount of time. (*Id.*, ¶ 18).

D. Efforts to Keep Moog's Flight Control Software Secret

Many Moog employees are required to sign Moog internal proprietary information agreements, as well as third party proprietary information agreements when working on certain project-specific applications. (*Id.*, ¶ 20). Every employee is required to periodically review and sign an acknowledgement in writing of the then-current Moog employee handbook (the "Employee Handbook"). (*Id.*, ¶ 21). Pilkington acknowledged its receipt and agreed to abide by its policies on July 30, 2012, and Kim acknowledged its receipt on January 21, 2013. (*Id.*, Ex. A). The employee handbook provides, among other things, that: 1) Moog employees will receive access to confidential and proprietary information; 2) disclosure to any outside party is prohibited, including after employment has been terminated; and 3) Moog employees may not retain any copies of Moog's confidential and proprietary information. (*Id.*, Ex. B at pp. 58-59).

Moog also has robust written policies regarding its confidential, proprietary, and trade secret information made available to every Moog employee, and Moog requires its software engineers to regularly complete trainings regarding company "trade secrets" which summarizes the contents of its written IP policies. (*Id.*, ¶ 24, Exs. C, D). Pilkington and Kim attended these trainings multiple times. (*Id.*, Ex. E). Moog also requires its departing employees to sign an exit form where each individual confirms they have been provided access to Moog's proprietary and trade secret information, have returned all Moog IP upon departure, and have not maintained access to any digital record of Moog. (Daly Dec., Ex. A at p. 3).

Platform is housed on a secure server at Moog's East Aurora, New York offices. Not all employees at Moog have access to the software database. (Hunter Dec. ¶ 25). Access to the software database is on a "need to know" basis that must be approved by the lead on software program. (*Id.*, ¶ 26). In order to have access to Platform and related project-specific software, a Moog employee would need five separate credentials. (*Id.*, ¶ 27). Further, certain US Government programs require heightened security credentials which take a long time to obtain.[1] (*Id.*, ¶ 65). Moog also has several physical security measures to safeguard its proprietary information, including controlled access into buildings, mandatory security screenings for all employees, and background checks before hiring. (*Id.*, ¶ 22). Finally, Moog source code files are designated "MOOG PROPRIETARY and CONFIDENTIAL INFORMATION" and contains restrictive language prohibiting its disclosure to third parties. (*Id.*, ¶ 29).

[1] Moog has obligations under its government contracts to implement extensive security measures to safeguard and protect sensitive information, including but not limited to, access restrictions, authentication, encryption, physical protections, and specific training for employees. Moog also employs additional requirements and protections for sensitive data for certain of its government customers.

E. Relevant Moog Team That Developed Platform

Gonzalo Rey (former Director of Engineering and Chief Technology Officer) and Sathya Achar (former Engineering Technical Fellow) were the first two Moog employees to sponsor and oversee the development of Moog Platform base software beginning in 2007. (Hunter Dec. ¶ 30). They have the most institutional and technical knowledge regarding the software, as well as its relationship with project-specific applications which sit on top of the base software. (*Id*.).

Michael Hunter and Todd Schmidt are two senior level engineers who have worked on and managed the programs that created Platform and related applications, since 2007. (Hunter Dec. ¶¶ 3-4) (Schmidt Dec. ¶¶ 3-4). Robert Alin Pilkington (former Senior Staff Engineer) was the lead architect on eRTOS. (Hunter Dec. ¶ 31). Pilkington reported to Hunter and Schmidt during his tenure at Moog. (Hunter Dec. ¶ 31) (Schmidt Dec. ¶ 24). Misook Kim was a Senior Staff Engineer who worked under Pilkington. (Hunter Dec. ¶ 31).

F. Moog and Skyryse's Initial Business Relationship

In 2018, Moog's Growth & Innovation Group (focused on finding new and innovative business opportunities for Moog outside of its existing business channels) began exploring a potential business opportunity with Skyryse. (Stoelting Dec., ¶ 7). Skyryse indicated it wanted offer on-demand helicopter transportation to the general public, through the use of automated flight system technology. (*Id*., ¶ 9). Under this proposed structure, Moog would provide the automated helicopter flight control systems (including flight control software, actuators, and computers), and Skyryse would install and implement this technology into their business. (*Id*.). This proposal was appealing to Moog, providing a new business channel that would capitalize on Moog's decades of experience in developing flight control systems. (*Id*.).

Moog and Skyryse entered into two separate Non-Disclosure Agreements on October 24, 2018 (the "2018 NDA") and March 15, 2019 (the "2019 NDA") (collectively, the "NDAs").

(Stoelting Dec. ¶¶ 12-13, Exs. A, B). Under those NDAs, the Parties agreed not to disclose any proprietary information disclosed by the other parties, refrain from any reverse engineering, and the receiving party of such information could only be used for the limited purpose of the contemplated engagement between Moog and Skyryse. (*Id.*, § 2).

Moog and Skyryse's business relationship was to be conducted in four separate phases. On May 31, 2019, the Parties entered into a [redacted]

On June 3, 2019, Moog and Skyryse entered into a corresponding [redacted]

G. Skyryse's Changes Its Business Model to Overlap with Moog's

Moog met its obligations and timely provided to Skyryse the deliverables under the SOW. (Stoelting Dec. ¶ 21). However, Skyryse's planned launch in October 2019 failed as it stopped its business operations, fired many of its employees, and pivoted its business model. (*Id.*, ¶ 22). In late 2019, Skyryse began advertising that it was offering an autonomous flight system as part of a flight control operating system. (*Id.*, ¶ 23). Skyryse called its flight operating system "Luna," which was very similar to Moog's name for its autonomous flight system previously discussed with Skyryse, "Lucy." (*Id.*). It became clear to Moog that Skyryse had now pivoted into developing exactly the technology that it had proposed engaging Moog to perform. (*Id.*).

On May 22, 2020, Skyryse issued a request for quote ("RFQ") to Moog. (Stoelting Dec. ¶ 24, Ex. E). Skyryse requested that Moog provide flight control computers and actuator systems for Skyryse to use and to implement Skyryse's flight control operating system software. (*Id*., ¶ 25). This was already an established line of business for Moog, so Moog's Growth & Innovation Group was reluctant to move forward. (*Id*.). Nonetheless, given the prior business relationship with Skyryse, and the fact that several former Moog employees worked at Skyryse, on September 22, 2020, Moog submitted a bid in response to Skyryse's RFQ for $46,195,870. (*Id*., ¶ 26, Ex. F). Skyryse advised Moog that its bid was too expensive and declined. (*Id*., ¶ 27). Phase 1 concluded, but the terms of the 2018 and 2019 NDAs were never terminated. (*Id*., ¶ 28).

H. Skyryse's Raiding of Moog's Employees

To date, Skyryse has hired 20 software engineers from Moog, with the majority of these departures occurring in the past few months. (Hunter Dec. ¶ 34). Rey was the first Moog employee to join Skyryse when he left Moog in 2017. (*Id*.). Achar joined Skyryse in January 2022, after advising Moog that he was retiring. (*Id*.). Pilkington left Moog on November 12, 2021 to join Skyryse. (*Id*.). These key, senior individuals are extremely familiar with Moog's Platform base software and related project-specific applications, as well as the more capable members of Moog's software engineering teams who worked on these programs. (*Id*., ¶ 35).

Kim left Moog on December 17, 2021 to join Skyryse. (*Id*., ¶ 34). Several additional software engineers have followed suit. Several additional software engineers have followed suit. Skyryse has reached out to a large number of software engineers at Moog, primarily targeted at Moog's Los Angeles-area office. (*Id*., ¶ 38).

While some engineers have remained loyal to Moog, Skyryse has aggressively recruited them as well. For example, in August 2021, Rey contacted Hunter and asked him to join

Skyryse. (*Id.*, ¶ 36). In January 2022, Pilkington reached out to Hunter asking him to join Skyryse. (*Id.*, ¶ 37). Pilkington advised Hunter that there was "urgency" at Skyryse. (*Id.*).

Similarly, on October 13, 2021, Rey contacted Schmidt to see if he would join Skyryse as lead engineer. (Schmidt Dec. ¶ 9). Rey told Schmidt something to the effect of: "You will become very wealthy." (*Id.*, ¶ 11). During a phone call, Rey advised Schmidt that Skyryse's goal was extracting flight control functions to an iPad type of interface, so that anyone who can use an iPad can fly a helicopter. (*Id.*, ¶ 10). Rey also advised that Skyryse wanted to provide an entire system that could fly an aircraft, including hardware and software components (*Id.*).

I. Substantial Data Theft of Moog's Most Proprietary Information

Moog recently discovered that on November 19, 2021, between the hours of 3:00 and 7:00 a.m. and from a remote location, former Moog employee Kim copied certain Moog data to an external hard drive. (Bagnald Dec., ¶¶ 8, 10). This event took place less than one month before Kim's last day at Moog, and less than one week after Pilkington, her supervisor, left Moog for Skyryse. (*Id.*). Kim copied 136,994 separate files:

Type	Number
Source Code	43,960
Spreadsheets	5,377
Documents	2,831
Executables	954
Images	9,003
MAP Files	2,010
Models	7,898
Object Files	1,026

Plain Text	4,613
Presentations	404
Misc.	20,655
SVN Logs	38,263
Total Files	**136,994**

(*Id*., ¶ 13). Kim used Pilkington's file path to copy the data onto the external hard drive. (Bagnald Dec. ¶ 14) (Hunter Dec. ¶ 47) (Schmidt Dec., ¶ 23). Employees working on Platform had their own "branch" or location on Moog's server, to store sensitive materials they needed access to. (*Id*.). The file path used by Kim was: "D:\Misook\ENG_Alin_Branch\Software…" (*Id*.). Kim had credentials to use her own file path, but instead used Pilkington's. (*Id*.).

Several Moog senior engineering employees have confirmed that Kim was very loyal and obedient to Pilkington, and would do anything he instructed. (Hunter Dec. ¶ 51) (Schmidt Dec. ¶¶ 24-25) (Lopez Dec., ¶ 6). Kim would not have accessed Pilkington's branch unless he expressly instructed her to do so. (*Id*.).

J. Nature and Value of the Copied Data

The scope of data copied by Kim is remarkable. Moog senior engineers Messrs. Hunter and Schmidt have analyzed the file log of data copied by Kim (the "File Log"). (Hunter Dec. ¶¶ 42-43) (Schmidt Dec. ¶¶ 18-19). The entire application layer for Platform was copied by Kim, meaning that 100% of the base Platform software and its code were copied. (Hunter Dec. ¶ 45) (Schmidt Dec. ¶ 21). All three iterations (commercial, military, motors) of Platform were copied, as well as test artifacts (*Id*.). Kim copied the entire application layer for seven project-specific applications, including six military projects. (*Id*.). This comprises all of the code, documentation, and related information regarding the composition, testing, and certification of

Platform and project-specific applications. (Hunter Dec. ¶ 46) (Schmidt Dec. ¶ 22) (Lopez Dec. ¶ 11). Additionally, in addition to source code, Kim copied Moog's trade secret checklists (76) and five documents from its SEPG repository. (Hunter Dec. ¶ 46). Kim essentially copied everything that Moog's flight control software engineering teams had worked on over the past 15 years. (Hunter Dec. ¶ 63) (Schmidt Dec. ¶ 27) (Lopez Dec. ¶ 14).

K. No Legitimate Purpose for Kim's Data Copying

There was no legitimate purpose for Kim's copying of Moog's proprietary, confidential, and trade secret information. Kim signed an exit form (the "Exit Form") on her last day at Moog, December 17, 2021, where she affirmed in writing that she had returned all Moog "TRADE SECRET/COMPANY CONFIDENTIAL INFO." (Daly Dec., Ex. A). The Exit Form also provides, among other things: 1) Kim "owes a fiduciary duty to Moog to not usurp any such corporate opportunity for [her] own benefit"; and 2) Kim affirms that she does "not maintain access to, or have possession of, any tangible or digital record of Moog IP-whether in hard copy or digital form—on any device, cloud, or digital storage facilities." (*Id*.).

Regardless, the standard way in which Moog employees worked on Platform-related projects would be connecting to Moog's server via remote virtual private network ("VPN"). (Hunter Dec. ¶ 27). All of the data copied by Kim is located on Moog's internal servers in East Aurora, New York. Even if Kim was working on a different Moog computer, she could access all the data she copied from Moog's Subversion network using her login credentials. (Schmidt Dec ¶ 32). Even if downloading data was necessary, a copy of the data would be stored to the user's hard drive on their laptop computer – not an external hard drive. (Hunter Dec. ¶ 48).

Further, in December 2021, Kim was working solely on a military program labeled herein as "Sensitive Government Program 2." (Hunter Dec. ¶ 54) (Schmidt Dec. ¶ 31) (Lopez Dec., ¶ 15). Kim was a software tester, not an engineer who wrote code. (Hunter Dec. ¶ 49).

Thus, even if Kim wanted to copy certain Moog data for legitimate business purposes, she would only have a need to copy certain verification and testing data related to Sensitive Government Program 2 (instead of the entire application layer for several projects she never touched). (Schmidt Dec. ¶ 31). To support legitimate business purposes, Kim would have needed, at most, to access only 0.5% of the total data that she copied on November 19, 2021. (*Id.*).

L. Kim Returns Two Hard Drives Which are Both Wiped Clean

When contacted by Moog, Kim engaged in a cover up in an attempt to mask her actions. On January 28, 2022, Moog informally requested that Kim return the company-issued external hard drive she had in her possession. (Bagnald Dec. ¶ 15). On January 31, 2022, Kim's sister who also works at Moog returned on Kim's behalf a hard drive to Moog. (*Id.*). However, a quick inspection of this device revealed it was not the device Kim used to copy Moog's data on November 19, 2021, ***and*** it had been completely wiped clean. (*Id.*, ¶¶ 11, 16-17).

On February 18, 2022, Moog sent a formal letter to Kim demanding that she return the external hard drive in question. (Daly Dec. ¶ 5, Ex. B) Kim called Moog's HR employee Jamie Daly, advising her that she had possession of the Moog external hard drive, and that she downloaded a large set of files in order to help Moog employees after her departure. (*Id.* ¶ 7). Kim claimed she needed the files for Sensitive Government Program 2. (*Id.*). She then volunteered that she had deleted all of the files on the drive. (*Id.*). The hard drive in question was eventually returned to Moog. (*Id.*, ¶ 8).[2]

[2] This explanation makes no sense because: 1) there was no plan or agreement for Kim to assist Moog employees after her departure; 2) at the time of departure, Kim was only working on testing related to Sensitive Government Program 2, and therefore was only involved in at most 0.5% of the total data she copied; 3) Kim returned a different hard drive the first time without any mention of the actual hard drive in question; and 4) Kim should have disclosed the data she copied on her Exit Form. (Hunter Dec. ¶¶ 52-57).

An expert forensic analysis was performed on Kim's two hard drives and two Moog-issued laptops which revealed: 1) the hard drive used to copy over 136,000 files of Moog's data had been intentionally formatted sometime after Kim's departure from Moog in such a manner that it is impossible to determine the contents of the drive or if any data was copied or transferred to another device; 2) Kim copied additional Moog data to the same hard drive on December 15, 2021, and 54 GB of data was deleted from one of Kim's computers just two days later; and 3) there is a third external hard drive used by Kim during the relevant period which has not been returned to Moog; and 4) the initial false hard drive returned by Kim's sister had been re-named in an effort to resemble the second hard drive which was used to actually copy Moog's data. (*See generally* Pixley Dec.). Further, the back covers of Kim's two Moog-issued laptop devices indicate they have been removed (allowing removal of its hard drives). (Johnnie Dec., ¶¶ 11-13, Exs. C, D).

M. Unmanned Helicopter Aviation Market and Barrier to Entry

Unmanned helicopter aviation, which both Moog and Skyryse are pursuing, is a new market with no industry leader. (Hunter Dec. ¶ 59). About 20 companies, including Moog and Skyryse, have entered the market and are rushing to become the market leader. (*Id.*). Whichever company wins that race will likely win a large portion of the market share just by being the first to market with a viable product. By stealing Moog's source code and other proprietary information underlying Platform and related applications, and crippling Moog's software engineering workforce, Skyryse has jumped to the front of this race to be first to market and has slashed Moog's tires along the way. This race against time underscores the irreparable harm faced by Moog because time cannot be unwound. If another party gained access to Moog's flight control software and related data, this would give that party a substantial advantage as it would save tens of millions of dollars and several years of developing, certifying, and testing that software. (*Id.*).

There is generally a high barrier to entry in the flight control software market. (*Id.*, ¶ 60). Companies that have an established, tested, and proven software and have successfully delivered on contracts before have a huge advantage in securing contracts from the government and other third parties. (*Id.*). Other companies would have to pay two to three times what Moog does to secure a flight control software contract because Moog has an established flight control operating system software. (*Id.*, ¶ 61). Moog wins many of the flight control projects that it bids on. (*Id.*).

If a third party such as Skyryse was able to obtain the entire code and underlying data to Moog's Platform software and related project-specific software, the large barrier to entry would be removed. (*Id.*, ¶ 63). This information in the hands of Skyryse removes a large barrier to entry and saves Skyryse tens of millions of dollars and decades of work. Some of the project-specific applications copied by Kim, including G280, are directly relevant to the line of business Skyryse is pursuing. (Hunter Dec. ¶ 61) (Schmidt Dec. ¶ 28).

Kim essentially copied every piece of data related to every flight control software and application that Moog has worked on over the past 15 years. (Hunter Dec. ¶ 63) (Schmidt Dec. ¶ 27). This information is truly priceless and represents the highest level of intelligence and wisdom of Moog's smartest architects of the past two decades. (Schmidt Dec. ¶ 27).

N. Level of Investment by Moog in its Flight Control Programs

Moog's investment of engineering time, money, and other resources into the development, testing, and certification of its programs and applications has been enormous. Moog has invested approximately [redacted] in developing testing, and certifying all three iterations of its Platform base software over the past 15 years. (Hunter Dec. ¶ 16). Moog has also invested approximately [redacted] in developing, testing, and certifying its aircraft project-specific software applications that sit on top of the Platform software. (*Id.*).

For context, Moog's flight control systems for a commercial aircraft (including software, hardware, actuation, hydraulics, etc.) typically cost between [redacted] for each type of aircraft, which in turn require over one million hours of software engineering and support staff time. (Schmidt Dec. ¶ 15). For example, Kim copied all data related to the eRTOS iteration of the Platform base software. (Lopez Dec. ¶ 11). [redacted] (*Id.* ¶ 13). Just writing the code for eRTOS took multiple years. (*Id.*). Once written, it still takes several additional years to verify, test, and certify the code under Federal Aviation Administration and other international governing body standards. (*Id.*). As another example, Kim copied all data related to Sensitive Government Program 1, [redacted] (*Id.* ¶ 12).

O. Reputational Harm and Loss of Goodwill

Kim's copying of Moog's proprietary software and related data has substantially damaged Moog's goodwill and reputation. (Hunter Dec. ¶ 67). Under every contract that Moog enters into for flight software development, Moog must notify its customers if certain proprietary or confidential data is copied or stolen. (*Id.*, ¶ 66). Moog is thus required to notify each of its customers, including the US Government, of Kim's theft of classified information. Moog has never before had to notify the US Government of a data theft regarding its software, and the US Government understandably reacts very negatively when its data is compromised. (*Id.*).

Moog's required disclosure will inevitably cause tremendous harm to Moog's reputation and goodwill in the industry because data and information security is of paramount concern in this industry, especially with the US Government. (*Id.* ¶ 67). Moog has historically been regarded as excellent and trustworthy in terms of data security and confidentiality. (*Id.*). Any notion that Moog is not careful with its customers' data will cause tremendous reputational harm and will likely cause Moog to lose future contracts that it otherwise would obtain. (*Id.*).

III. <u>ARGUMENT</u>

A. Good Cause for Expedited Discovery

Upon good cause shown, a Court may order early or expedited discovery prior to the Rule 26(f) conference. FED. R. CIV. P. 26(d); *Ayyash v. Bank Al-Madina*, 233 F.R.D. 325, 326 (S.D.N.Y. 2005). This court applies a "flexible standard of reasonableness and good cause in determining whether to grant a party's expedited discovery request." *Id.* at 327; *Stern v. Cosby*, 246 F.R.D. 453, 457 (S.D.N.Y. 2007). When, as here, expedited discovery is requested in connection with a preliminary injunction hearing, expedited discovery should be granted. *See, e.g.*, *Delphine Software Int'l v. Elec. Arts, Inc.*, No. 99 CIV. 4454 AGAS, 1999 WL 627413, at *3 (S.D.N.Y. Aug. 18, 1999); *New York by Schneiderman v. Griepp*, No. 17CV3706CBAJO, 2017 WL 3129764, at *1 (E.D.N.Y. July 20, 2017) (granting expedited discovery to a defendant in order to prepare for preliminary injunction hearing).

District courts in this Circuit have granted expedited discovery when, as here, plaintiffs can show that the actions of defendants are causing irreparable harm, including "loss of goodwill, negative effect on profitability and damage to its relationships with its direct clients/customers." *N. Atl. Operating Co. v. Evergreen* Distributors, LLC, 293 F.R.D. 363, 368 (E.D.N.Y. 2013) (granting expedited discovery finding good cause where plaintiff showed irreparable harm and that expedited discovery could help to avoid irreparable harm); *Oneida Grp. Inc. v. Steelite Int'l U.S.A. Inc.*, No. 17CV0957ADSAKT, 2017 WL 1954805, at *23 (E.D.N.Y. May 10, 2017) (finding good cause where a plaintiff showed that "it may suffer irreparable harm").

The facts here clearly indicate that Moog has already suffered and will continue to suffer irreparable harm if Defendants are not enjoined from further misappropriating and using Moog's trade secret, confidential and proprietary information, and from further breaching or interfering with applicable agreements between Moog and Defendants. Moog requires the following reasonable expedited discovery from Defendants in order to adequately prepare for the preliminary injunction hearing and prevent further irreparable harm to Moog:

- Depositions of Kim, Pilkington, Rey, and a Person Most Knowledgeable regarding Skyryse's software engineering team and practices (pursuant to Fed. R. Civ. P. 30(b)(6));
- Documents relating to Skyryse's access, use, and/or disclosure of the Moog data copied by Ms. Kim on November 19, 2021;
- Documents and communications between Skyryse, Kim and Pilkington regarding the Moog data that was copied on November 19, 2021;
- Documents and communications between Skyryse and any of the 21 former Moog employees who have left for Skyryse, before such individuals started working at Skyryse;
- Documents and communications between Skyryse, Rey, and Pilkington, on the one hand, and Kim, on the other hand, regarding Moog or any of its confidential information;
- Documents related to the development of Skyryse's flight control systems and software after its initial business relationship with Moog in 2018;
- Internal Skyryse documents related to communications and solicitations of Moog employees;
- Internal Skyryse documents related to Moog's flight control systems and software; and
- Documents related to Skyryse's representations to actual or prospective investors regarding its business plans or potential launch dates.

While Moog's preview of its anticipated discover is not necessary for the purposes of this Motion, it has identified the above categories so the Court can confirm that Moog's discovery will be narrowly tailored to Moog's claims and relief sought. *See, e.g.*, *Philip Morris USA Inc. v. Garrow*, No. 8:13-CV-1549 GTS, 2013 WL 6844347, at *2 (N.D.N.Y. Dec. 17, 2013) (granting expedited discovery without specific discovery requests, including, among other things, "up to 15 interrogatories" and "requests for production.").

Courts in this circuit have granted expedited discovery in cases where plaintiffs brought claims similar to those that Moog brings here. *See, e.g.*, *In re Document Techs. Litig.*, No. 17-CV-2405, 2017 WL 4350597, at *3 (S.D.N.Y. June 27, 2017) (noting that district court granted expedited discovery at plaintiff's request in case involving claim for misappropriation of trade secrets); *OMG Fid., Inc. v. Sirius Techs., Inc.*, 239 F.R.D. 300, 301 (N.D.N.Y. 2006) (granting expedited discovery to plaintiff in case involving claim for misappropriation of trade secrets); *Ticor Title Ins. Co. v. Cohen*, 173 F.3d 63, 67 (2d Cir. 1999) (noting that district court granted expedited discovery in case involving claim for breach of restrictive covenant). Likewise, expedited discovery is warranted here.

Further, expedited discovery is also warranted where there are legitimate concerns regarding the potential spoliation of evidence. *See, e.g.*, *Delphine Software Int'l*, 1999 WL 627413, at *3 (granting expedited discovery and noting "legitimate concerns" that "evidence of any misappropriation will disappear"). Here, Defendants have already engaged in tortious and unfair conduct, and Defendant Kim has already engaged in the deletion or destruction of evidence through the admitted deletion of the Moog data that she copied to the external hard drive on November 19, 2021 (which was later confirmed by the forensic inspection).

Under the facts presented here, expedited discovery is especially critical because Moog must understand immediately whether and to what extent Skyryse has accessed, used, or disclosed the substantial confidential and trade secret data that was stolen by Ms. Kim on November 19, 2021. Moog is also entitled to discover underlying communications between Skyryse, Pilkington, and Kim regarding the conduct and coordinated data theft described above. Consequently, there is a risk of further unauthorized use, disclosure or dissemination of Moog's trade secrets by Defendants, and such a risk "is sufficient to give rise to a showing of irreparable harm supporting preliminary injunctive relief." *Asa v. Pictometry Int'l Corp.*, 757 F. Supp. 2d 238, 246 (W.D.N.Y. 2010). In its accompanying Motion for Temporary Restraining Order/Preliminary Injunction, Moog has demonstrated irreparable harm caused by Defendants, and Defendants' further misappropriation of trade secrets will result in loss of goodwill, sales, and market share without injunctive relief. *See, e.g.*, *Fabkom, Inc. v. R.W. Smith & Assocs., Inc.*, No. 95 CIV. 4552 (MBM), 1996 WL 531873, at *5 (S.D.N.Y. Sept. 19, 1996); *Sylmark Holdings Ltd. v. Silicone Zone Int'l Ltd.*, 5 Misc. 3d 285, 299 (N.Y. Sup. Ct. 2004); *PLC Trenching Co., LLC v. Newton*, No. 6:11-CV-0515, 2011 WL 13135653, at *3 (N.D.N.Y. Dec. 12, 2011). Evidence that Kim has already improperly disclosed Moog's trade secrets to Skyryse, which Moog cannot obtain without expedited discovery, is absolutely imperative, as it "demonstrates that the use of [plaintiff's] intellectual property for [defendant's] own purposes to the [plaintiff's] detriment is a risk that cannot be dismissed as remote." *Secured Worldwide LLC v. Kinney*, No. 15 CIV. 1761 CM, 2015 WL 1514738, at *12 (S.D.N.Y. Apr. 1, 2015).

In sum, there is good cause for granting Moog expedited discovery: (i) because the issues presented in this case are time sensitive in nature, (ii) because the parties need to prepare for a preliminary injunction hearing, (iii) because expedited discovery will protect Moog from further imminent irreparable injury, and (iv) because it is a reasonable and necessary measure to prevent against further deletion or destruction of evidence.

B. Defendants Will Not Be Prejudiced by Expedited Discovery, and Plaintiffs Would Be Prejudiced if Expedited Discovery Were Not Granted

Where considering a grant of expedited discovery, district courts in this Circuit consider the prejudice to either party if the motion is granted or denied. *United States v. Erie Cnty.*, No. 09-cv-849S, 2010 U.S. Dist. LEXIS 144503, *12 (W.D.N.Y. March 6, 2010). Part of this inquiry is considering the likelihood that the requested expedited discovery would eventually take place in any event. *Id*. Where, as here, the requested discovery will "in all likelihood occur eventually" and the "plaintiff contemplates a motion for a preliminary injunction," on balance, the "plaintiff will potentially be unfairly prejudiced should [the Court] not permit [expedited] discovery to go forward." *OMG Fid., Inc. v. Sirius Techs., Inc.*, 239 F.R.D. 300, 305 (N.D.N.Y. 2006). Indeed, district courts in this Circuit have held that "where an expedited discovery request is made in contemplation of the filing of a motion for preliminary injunction, the denial of the request prejudices the moving party." *Erie Cnty.*, 2010 U.S. Dist. LEXIS 144503 at *12.

Here, it is critical that Moog be permitted to conduct expedited discovery in order to gather admissible evidence for presentation at the hearing on Presidio's motion for preliminary injunction. Defendants will not be prejudiced by expedited discovery, as responding to these demands is something that Defendants would be required to do shortly in this litigation in any event, and the requested discovery is narrowly tailored to discovery necessary to support Moog's Motion for a Preliminary Injunction.

IV. <u>CONCLUSION</u>

Moog has demonstrated good cause for its reasonable request for expedited discovery in connection with Moog's Motion for a Preliminary Injunction. Moog has further demonstrated that Moog will be prejudiced without expedited discovery, while there would not be significant prejudice to Defendants were expedited discovery granted. Accordingly, Moog respectfully requests that Moog's Motion for Expedited Discovery be granted.

Dated: New York, New York
March 7, 2022

SHEPPARD, MULLIN, RICHTER &
HAMPTON LLP
Attorneys for Plaintiff Moog Inc.

By: s/Rena Andoh
Rena Andoh
Travis J. Anderson (*pro hac vice* forthcoming)
Tyler E. Baker (*pro hac vice* forthcoming)
Kazim A. Naqvi (*pro hac vice* forthcoming)
30 Rockefeller Plaza
New York, New York 10112
Telephone: (212) 653-8700'

and

HODGSON RUSS LLP

By: s/Robert Fluskey
Robert J. Fluskey, Jr.
Melissa N. Subjeck
Pauline T. Muto
The Guaranty Building
140 Pearl Street, Suite 100
Buffalo, New York 14202
(716) 856-4000